



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/827,226	04/05/2001	Marcus Wong	1	6211

7590

12/28/2005

David J. Gaskey  
Carison, Gaskey & Olds, PC  
400 West Maple Road  
Suite #350  
Birmingham, MI 48009

EXAMINER

SHIFERAW, ELENI A

ART UNIT

PAPER NUMBER

2136

DATE MAILED: 12/28/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

**Office Action Summary**

Application No.

09/827,226

Applicant(s)

WONG, MARCUS

Examiner

Eleni A. Shiferaw

Art Unit

2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 14 November 2005.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-20 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☐ Claim(s) \_\_\_\_\_ is/are rejected.
- 7) ☒ Claim(s) 1-20 is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)                        | 4) <input type="checkbox"/> Interview Summary (PTO-413)                     |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)               | Paper No(s)/Mail Date. _____  |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| Paper No(s)/Mail Date <u>11/8/2004</u> .   | 6) <input type="checkbox"/> Other: _____                                    |

**DETAILED ACTION**

1. Applicant's arguments for Pre-Appeal Brief Review have been fully considered but are moot in view of the new ground(s) of rejection.
2. Claims 1-20 are pending.

***Claim Rejections - 35 USC § 102***

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4. Claims 1-20 are rejected under 35 U.S.C. 102(b) as being anticipated by Hwang (IEEE '99, Dynamic Participation in a Secure Conference Scheme for Mobile communications).

Regarding claims 1 and 13, Hwang teaches a method of providing secure communications between a first wireless unit and a second wireless unit, said method comprising the step of:

providing a common key value to a first wireless unit (page 1471 col. 1 lines 17-24; *trusted network center (NC) generating and providing common key to the first wireless terminal (TI)*) for use in secure communications over at least one wireless communications system between said first wireless unit and said second wireless unit having said common key (page 1471 col. 1 lines 19-20 and page 1469 section I paragraph 3; *any participant (second or third terminals) gets common key, for secure mobile communications without the communication unit*

*involving to encrypt/decrypt message exchanged between the terminals).*

Regarding claims 2 and 14, Hwang teaches the method wherein said step of providing comprising the steps of:

generating a first key value corresponding to said first wireless unit (page 1470 section II; *terminal-1 with key  $e$  ( $AK1$ ) ...that is used to request session key from network center, and Applicant Admitted Prior Art (AAPA) explains root key/ $A\_key/AK1$ , on page 3-5, as a well-known*);

generating a common key value (Hwang page 1470 steps 7-9;  $CK = (Q \cdot 2^2 + R) \bmod ri$ );  
and

sending said common key value to said first wireless unit using said first key value (Hwang page 1470 steps 8-9; *Ti obtains encrypted CK*).

Regarding claims 3 and 15, Hwang teaches the method comprising the steps of:

generating a second key value corresponding to said second wireless unit (page 1470 section II; *terminal-i with key  $e$  ( $AKi$ ) ...that is used to request session key from network center, and Applicant Admitted Prior Art (AAPA) explains root key/ $A\_key/AK2$ , on page 3-5, as a well-known*); and

sending said common key value to said second wireless unit using said second key value (Hwang page 1470 steps 8-9; *Ti obtains encrypted CK from network center*).

Regarding claims 4 and 16, Hwang teaches the method wherein said step of generating comprises the step of:

generating said first key value as a function of a first root key known only at said first wireless unit and a home wireless communications system for said first wireless unit (page 1470-1471 section II; and also *Applicant Admitted Prior Art (AAPA) explains first key value as a function of a first root key known at element 50 and 54, on page 4-5, as a well-known*).

Regarding claim 5, Hwang teaches the method wherein said step of generating comprises the step of:

generating said second key value as a function of a second root key known only at said second wireless unit and at a home wireless communications system for said second wireless unit (page 1470-1471 section II; and also *Applicant Admitted Prior Art (AAPA) explains second key value as a function of a second root key known at element 52 and 54, on page 4-5, as a well-known*).

Regarding claim 6, Hwang teaches the method wherein said step of providing comprises the steps of:

encrypting said common key using said first key value (page 1470 steps 7-9; *common key is encrypted using NC's key*); and

transmitting said common key encrypted with said first key value to said first wireless unit (page 1470-1471 section II; *encrypted CK is transmitted to Ti*);

Regarding claim 7, Hwang teaches the method wherein said step of providing comprises the steps of:

encrypting said common key with said second key value (page 1470 steps 7-9; *common key is encrypted using NC's key according to next terminal*); and

transmitting said common key encrypted with said second key value to said second wireless unit (page 1470 steps 7-9; *transmitting encrypted common key to Ti*).

Regarding claim 8, Hwang teaches the method wherein said step of generating said common key value comprises the steps of:

generating said common key as a function of at least one of said first key value and said second key value (page 1470-1471 section II; *common keys are generated as function of Ni key values*).

Regarding claims 9 and 18, Hwang teaches the method comprising the step of:

generating/receiving said common key as an encryption key (page 1471 col. 1 lines 3-24).

Regarding claims 10 and 19, Hwang teaches the method comprising the step of:

generating/receiving said common key as a session key (page 1470-1471 section II).

Regarding claims 11 and 20, Hwang teaches the method comprising the step of:

generating a first session key value as a function of a first root key known only at said first wireless unit and a home wireless communications system for said first wireless unit (page 1470-1471 section II; and also *Applicant Admitted Prior Art (AAPA) explains first session key as a function of a first root key known at element 50 and 54, on page 4-5, as a well-known*); and

generating/receiving said common key as a session encryption key being a function of at least said first session key value (page 1470-1471; *common session key is generated and received by terminals for secure mobile communication*).

Regarding claim 12, Hwang teaches the method comprising the steps of:

mutually producing said common key by a first wireless communications system for said first wireless communications system and a second wireless communications system for said second wireless unit (page 1470 fig. 1).

Regarding claim 17, Hwang teaches the method wherein said step of providing comprises the steps of:

decrypting said common key using said first key value (page 1470 step 4).

5. Claims 1 and 13 are also rejected under 35 U.S.C. 102(b) as being anticipated by Hwang '92, (IEEE 1992, Scheme for secure digital mobile communications based on symmetric key Cryptography).

Regarding claims 1 and 13, Hwang '92 discloses a method of providing secure communications between a first wireless unit and a second wireless unit, said method comprising the step of:

providing a common key value to a first wireless unit for use in secure communications over at least one wireless communications system between said first wireless unit and said second wireless unit having said common key (page 423 section II; *network center provides session symmetric key & nonce to the mobile unit-1...mobile unit-1 decrypts the encrypted session symmetric key & nonce and compares the nonce unit-1 sent with received and if match, unit-1 encrypts the message using symmetric session key and sends the encrypted message & unit-2 nonce to mobile user-2.... unit-2 authenticates the nonce same as unit-1 and decrypts the encrypted message sent from user-1 using symmetric session key and mobile unit-1 and unit-2 are securely communicated without the network center encrypting and decrypting messages exchanged between the units and/or no significant amount of processing by the network center is required to encrypt/decrypt data sent between the first and second mobile units*).

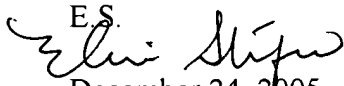
### *Conclusion*


6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Eleni A. Shiferaw whose telephone number is 571-272-3867. The examiner can normally be reached on Mon-Fri 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.



Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

E.S.  
  
December 24, 2005

  
AYAZ SHEIKH  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100